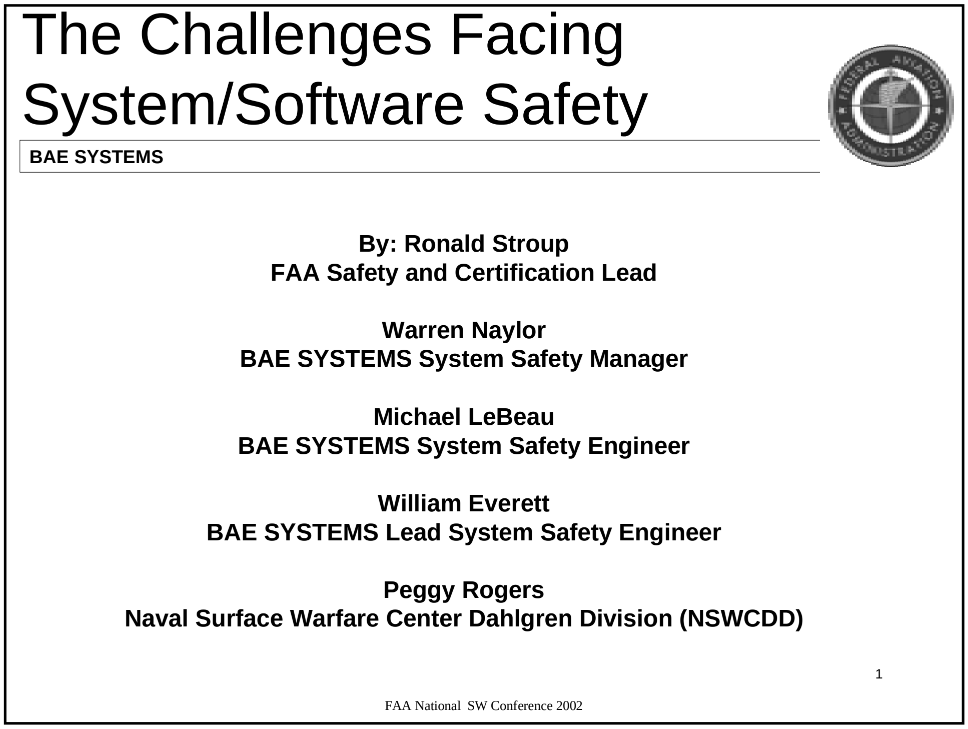


The Challenges Facing System/Software Safety

BAE SYSTEMS

By: Ronald Stroup
FAA Safety and Certification Lead

Warren Naylor
BAE SYSTEMS System Safety Manager

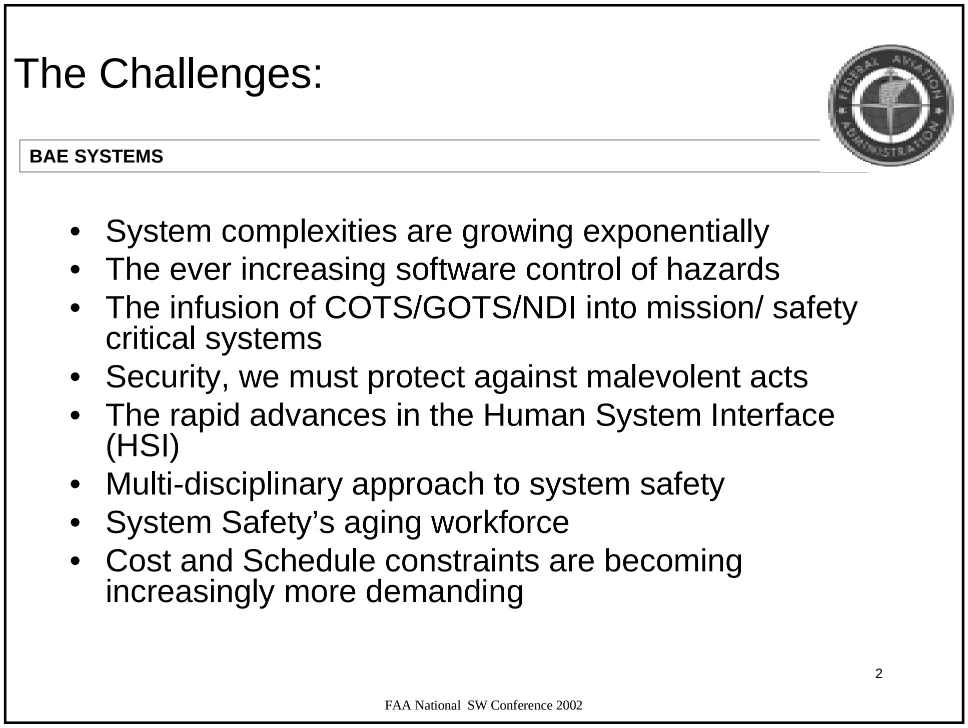
Michael LeBeau
BAE SYSTEMS System Safety Engineer

William Everett
BAE SYSTEMS Lead System Safety Engineer

Peggy Rogers
Naval Surface Warfare Center Dahlgren Division (NSWCDD)

1

FAA National SW Conference 2002



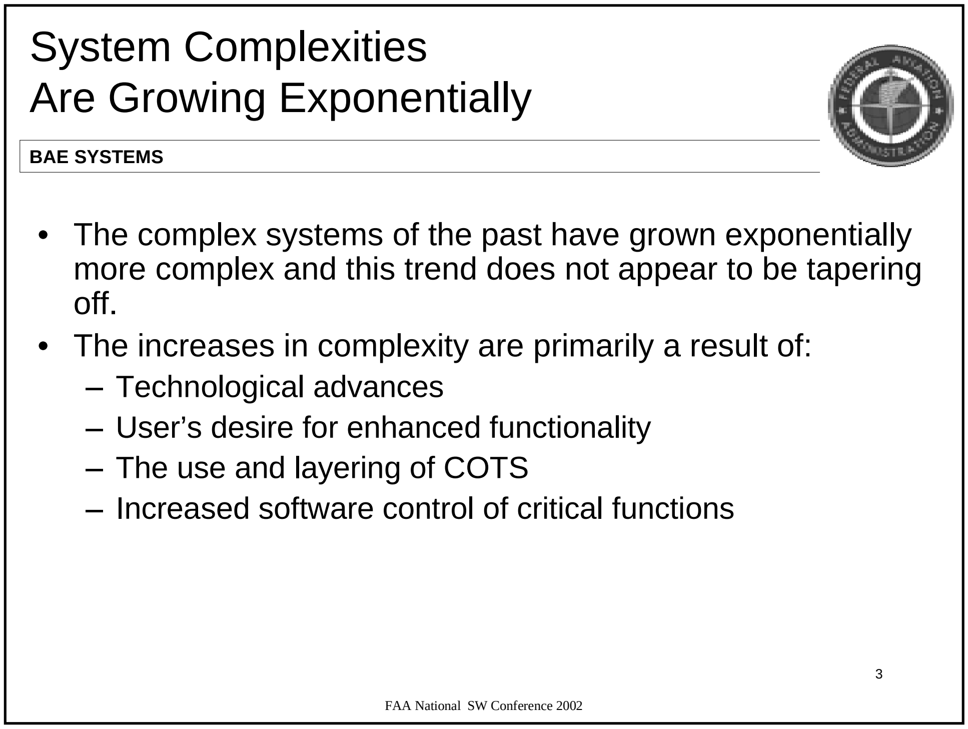
The Challenges:

BAE SYSTEMS

- System complexities are growing exponentially
- The ever increasing software control of hazards
- The infusion of COTS/GOTS/NDI into mission/ safety critical systems
- Security, we must protect against malevolent acts
- The rapid advances in the Human System Interface (HSI)
- Multi-disciplinary approach to system safety
- System Safety’s aging workforce
- Cost and Schedule constraints are becoming increasingly more demanding

2

FAA National SW Conference 2002



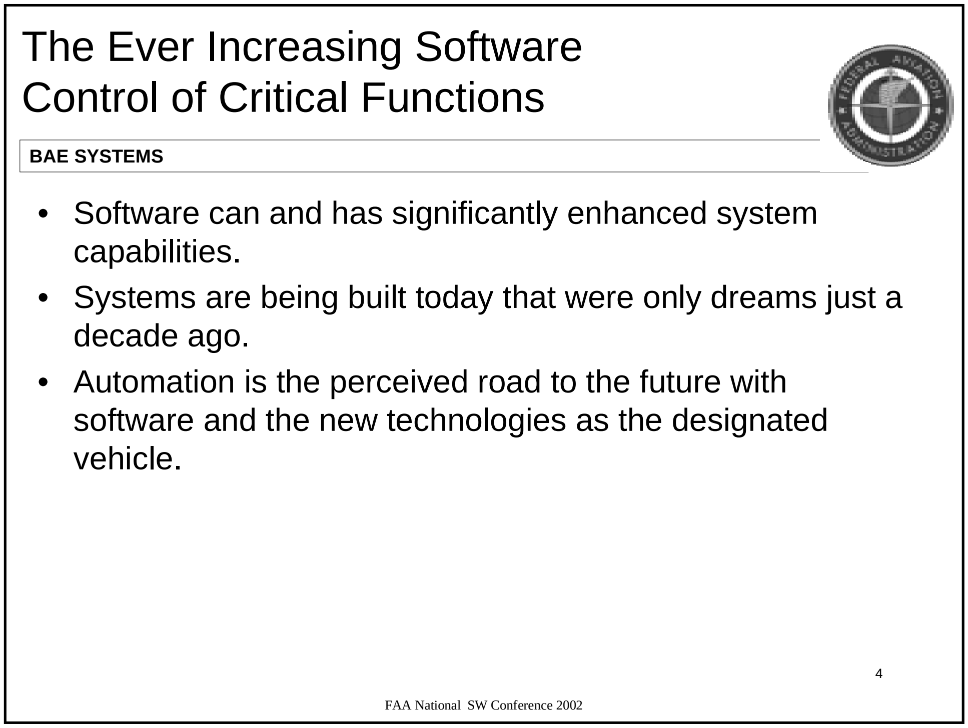
System Complexities Are Growing Exponentially

BAE SYSTEMS

- The complex systems of the past have grown exponentially more complex and this trend does not appear to be tapering off.
- The increases in complexity are primarily a result of:
  – Technological advances
  – User’s desire for enhanced functionality
  – The use and layering of COTS
  – Increased software control of critical functions

3

FAA National SW Conference 2002



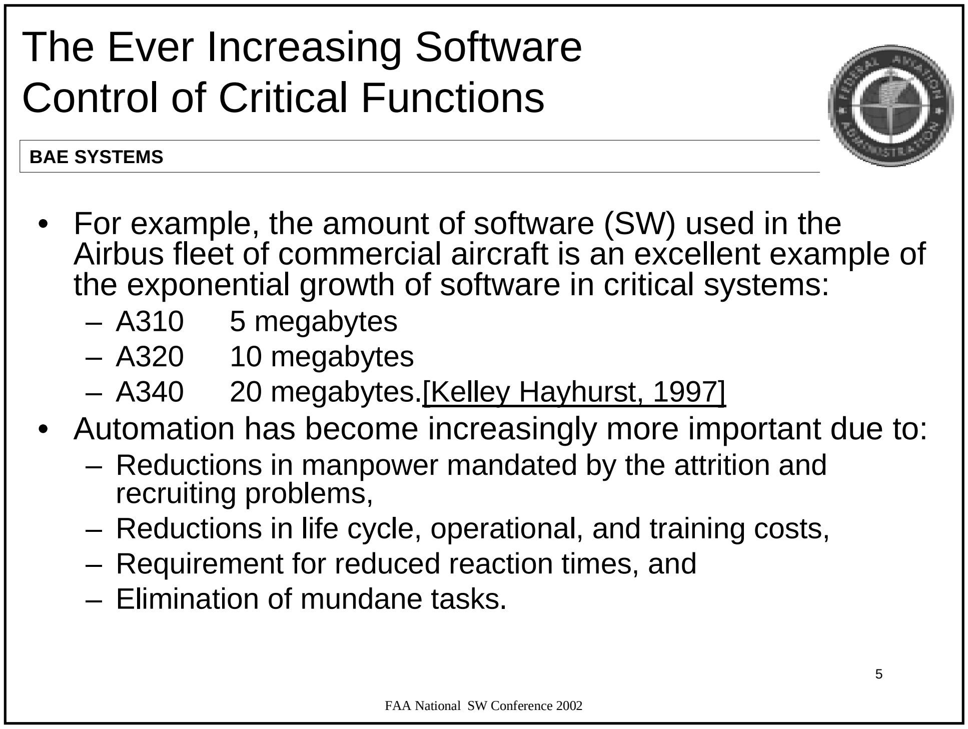
The Ever Increasing Software Control of Critical Functions

BAE SYSTEMS

- Software can and has significantly enhanced system capabilities.
- Systems are being built today that were only dreams just a decade ago.
- Automation is the perceived road to the future with software and the new technologies as the designated vehicle.

4

FAA National SW Conference 2002



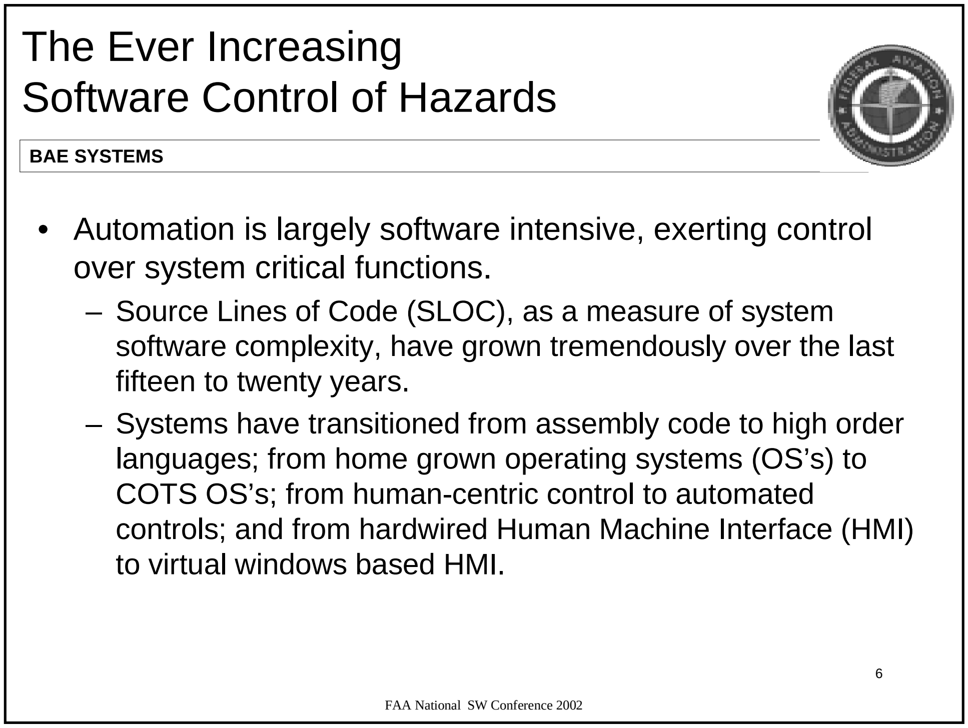
The Ever Increasing Software Control of Critical Functions

BAE SYSTEMS

- For example, the amount of software (SW) used in the Airbus fleet of commercial aircraft is an excellent example of the exponential growth of software in critical systems:
  - A310 5 megabytes
  - A320 10 megabytes
  - A340 20 megabytes.[Kelley Hayhurst, 1997]
- Automation has become increasingly more important due to:
  - Reductions in manpower mandated by the attrition and recruiting problems,
  - Reductions in life cycle, operational, and training costs,
  - Requirement for reduced reaction times, and
  - Elimination of mundane tasks.

5

FAA National SW Conference 2002



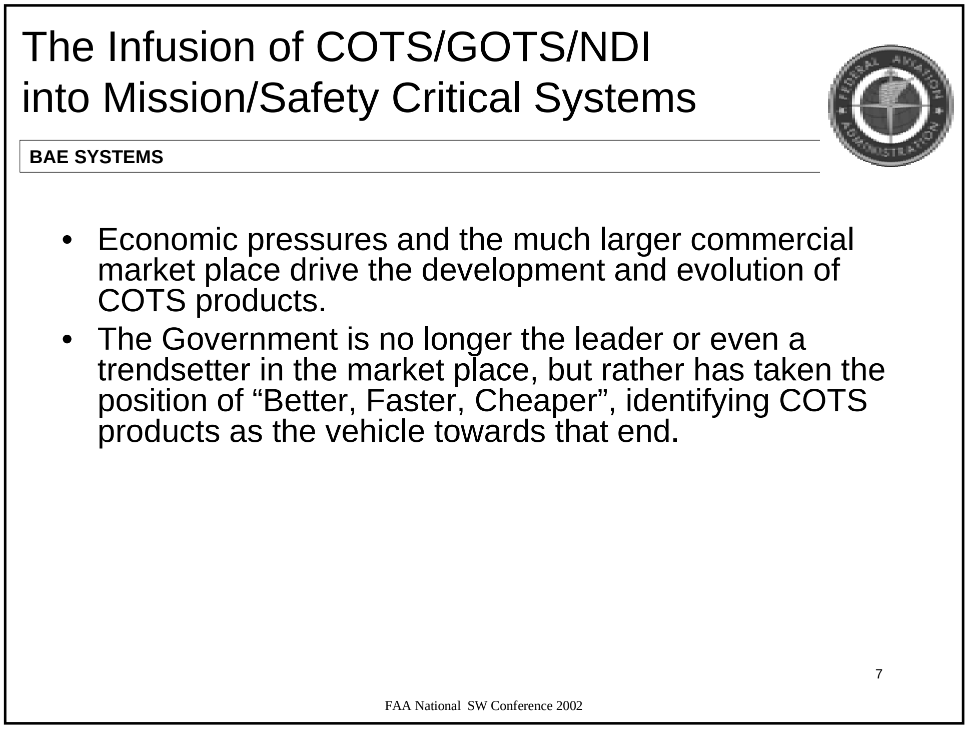
The Ever Increasing Software Control of Hazards

BAE SYSTEMS

- Automation is largely software intensive, exerting control over system critical functions.
  - Source Lines of Code (SLOC), as a measure of system software complexity, have grown tremendously over the last fifteen to twenty years.
  - Systems have transitioned from assembly code to high order languages; from home grown operating systems (OS's) to COTS OS's; from human-centric control to automated controls; and from hardwired Human Machine Interface (HMI) to virtual windows based HMI.

6

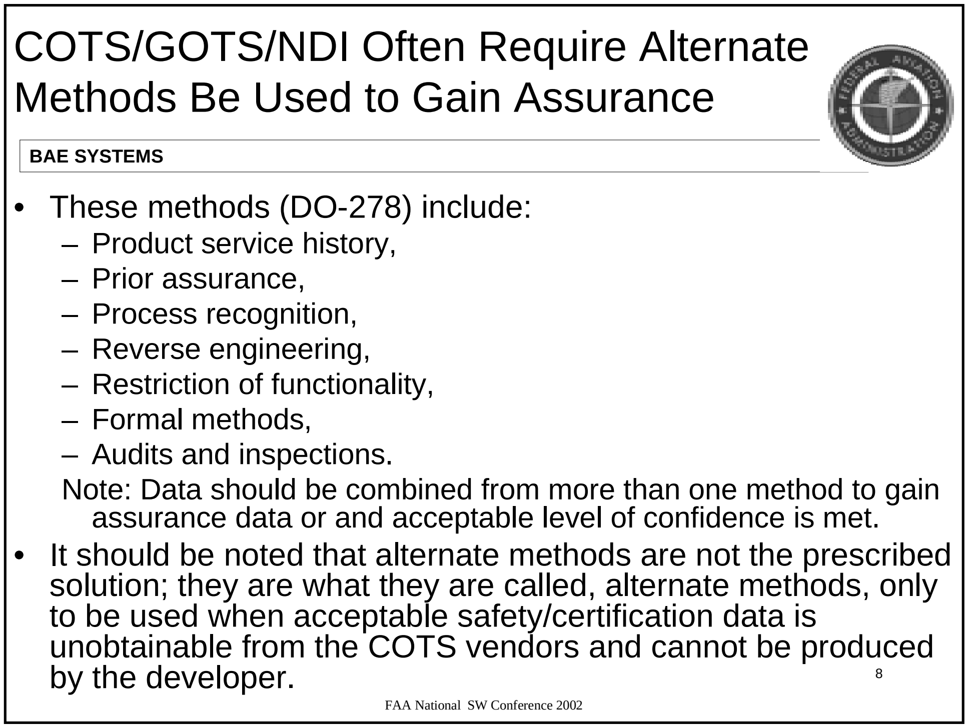
FAA National SW Conference 2002



The Infusion of COTS/GOTS/NDI into Mission/Safety Critical Systems

BAE SYSTEMS

- Economic pressures and the much larger commercial market place drive the development and evolution of COTS products.
- The Government is no longer the leader or even a trendsetter in the market place, but rather has taken the position of “Better, Faster, Cheaper”, identifying COTS products as the vehicle towards that end.

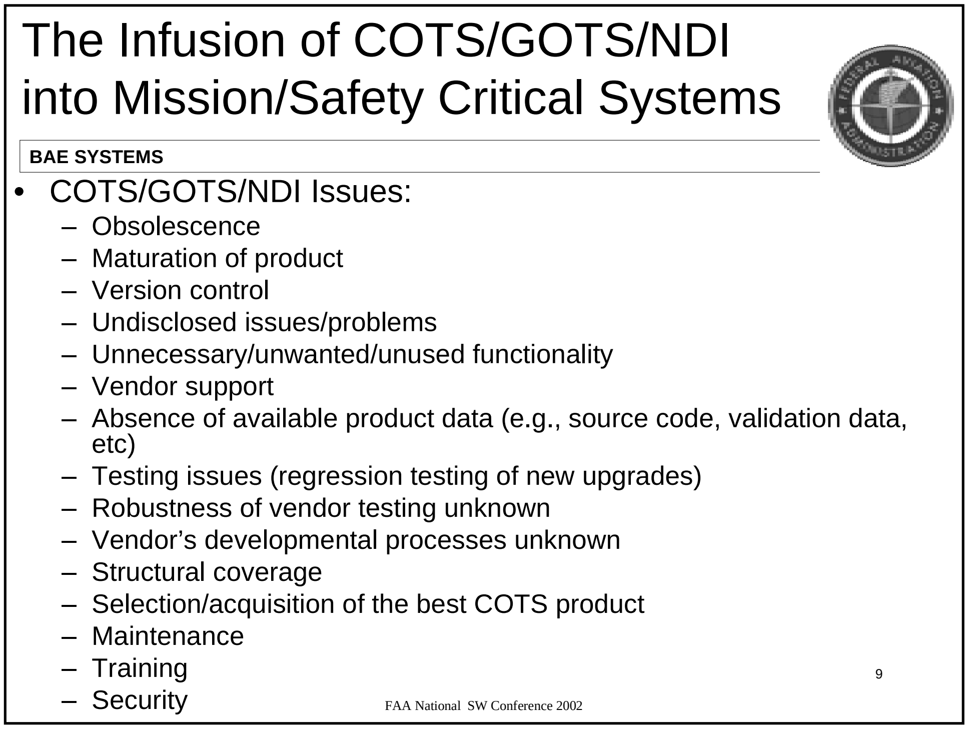


COTS/GOTS/NDI Often Require Alternate Methods Be Used to Gain Assurance

BAE SYSTEMS

- These methods (DO-278) include:
  - Product service history,
  - Prior assurance,
  - Process recognition,
  - Reverse engineering,
  - Restriction of functionality,
  - Formal methods,
  - Audits and inspections.

  Note: Data should be combined from more than one method to gain assurance data or and acceptable level of confidence is met.
- It should be noted that alternate methods are not the prescribed solution; they are what they are called, alternate methods, only to be used when acceptable safety/certification data is unobtainable from the COTS vendors and cannot be produced by the developer.



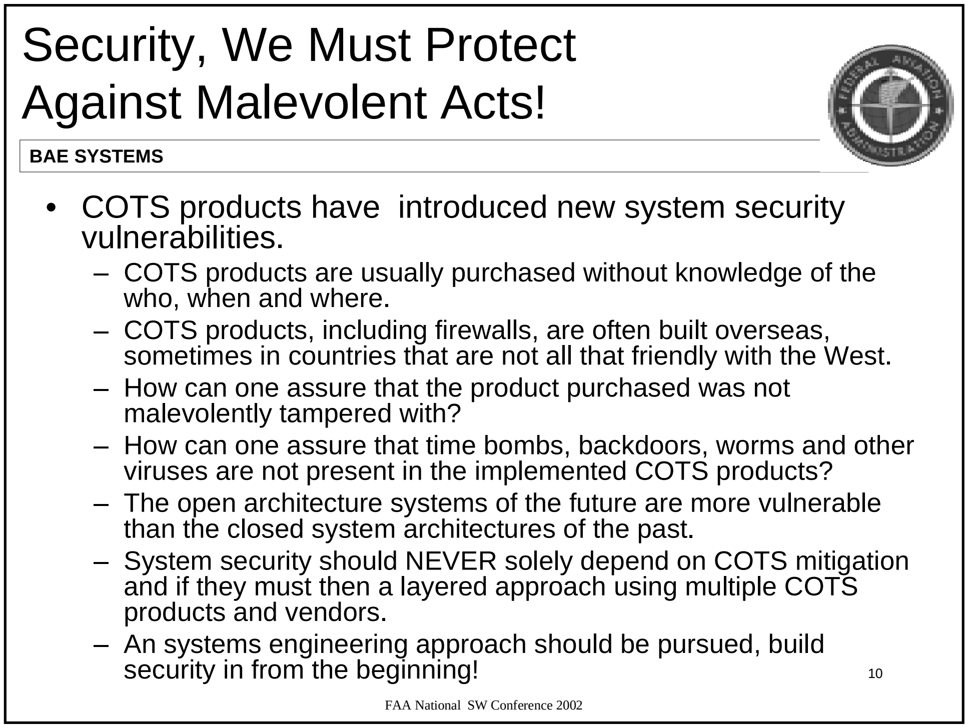
The Infusion of COTS/GOTS/NDI into Mission/Safety Critical Systems

BAE SYSTEMS

- COTS/GOTS/NDI Issues:
  - Obsolescence
  - Maturation of product
  - Version control
  - Undisclosed issues/problems
  - Unnecessary/unwanted/unused functionality
  - Vendor support
  - Absence of available product data (e.g., source code, validation data, etc)
  - Testing issues (regression testing of new upgrades)
  - Robustness of vendor testing unknown
  - Vendor's developmental processes unknown
  - Structural coverage
  - Selection/acquisition of the best COTS product
  - Maintenance
  - Training
  - Security

9

FAA National SW Conference 2002



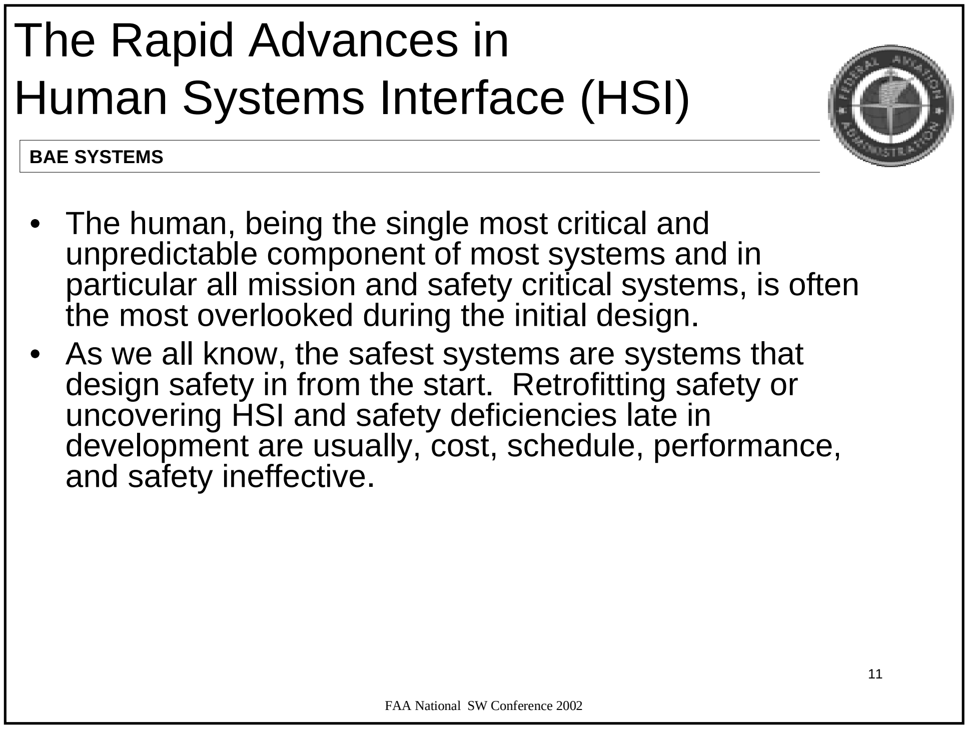
Security, We Must Protect Against Malevolent Acts!

BAE SYSTEMS

- COTS products have introduced new system security vulnerabilities.
  - COTS products are usually purchased without knowledge of the who, when and where.
  - COTS products, including firewalls, are often built overseas, sometimes in countries that are not all that friendly with the West.
  - How can one assure that the product purchased was not malevolently tampered with?
  - How can one assure that time bombs, backdoors, worms and other viruses are not present in the implemented COTS products?
  - The open architecture systems of the future are more vulnerable than the closed system architectures of the past.
  - System security should NEVER solely depend on COTS mitigation and if they must then a layered approach using multiple COTS products and vendors.
  - An systems engineering approach should be pursued, build security in from the beginning!

10

FAA National SW Conference 2002



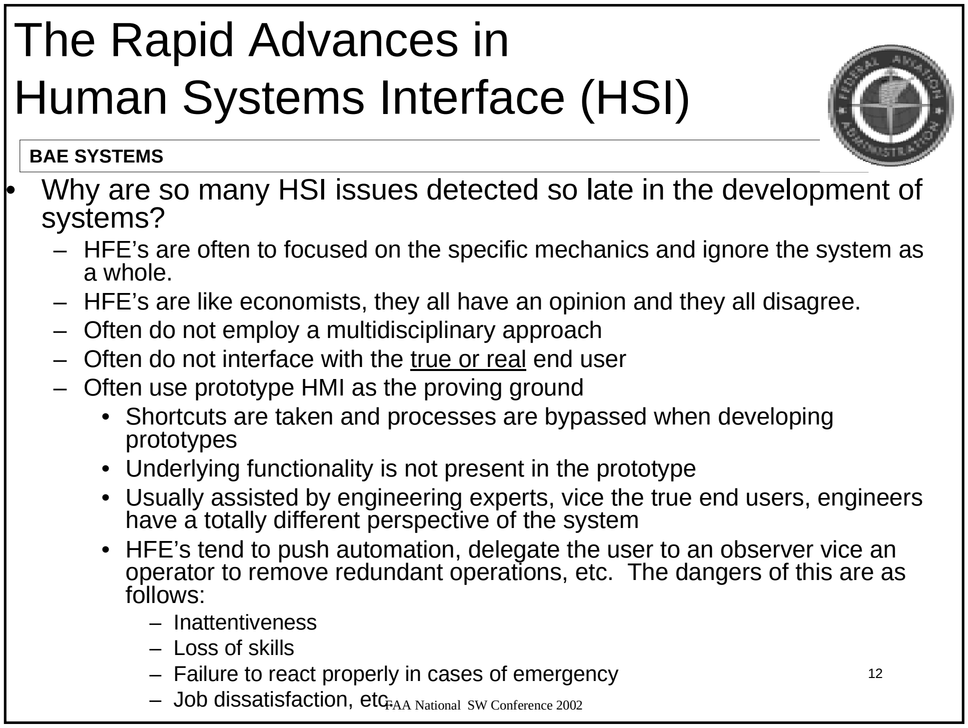
The Rapid Advances in Human Systems Interface (HSI)

BAE SYSTEMS

- The human, being the single most critical and unpredictable component of most systems and in particular all mission and safety critical systems, is often the most overlooked during the initial design.
- As we all know, the safest systems are systems that design safety in from the start. Retrofitting safety or uncovering HSI and safety deficiencies late in development are usually, cost, schedule, performance, and safety ineffective.

11

FAA National SW Conference 2002



The Rapid Advances in Human Systems Interface (HSI)

BAE SYSTEMS

- Why are so many HSI issues detected so late in the development of systems?
  - HFE’s are often to focused on the specific mechanics and ignore the system as a whole.
  - HFE’s are like economists, they all have an opinion and they all disagree.
  - Often do not employ a multidisciplinary approach
  - Often do not interface with the <u>true or real</u> end user
  - Often use prototype HMI as the proving ground
    - Shortcuts are taken and processes are bypassed when developing prototypes
    - Underlying functionality is not present in the prototype
    - Usually assisted by engineering experts, vice the true end users, engineers have a totally different perspective of the system
    - HFE’s tend to push automation, delegate the user to an observer vice an operator to remove redundant operations, etc. The dangers of this are as follows:
      - Inattentiveness
      - Loss of skills
      - Failure to react properly in cases of emergency
      - Job dissatisfaction, etc.

12

FAA National SW Conference 2002

On the Lighter Side

BAE SYSTEMS

- Conflicting requirements?
- Failure to look at the system in a systems context.
- Did not employ a multidisciplinary approach.

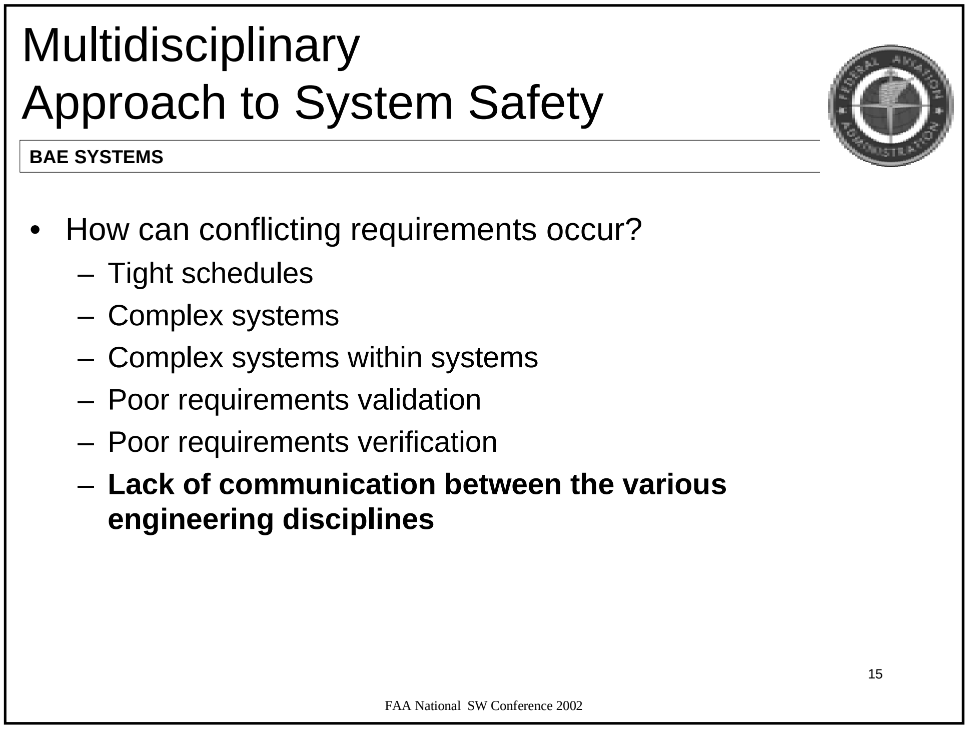
WHAT'S GOING ON?
AL FELL OFF A LADDER!
©2001 CREATORS SYNDICATE, INC. WWW.CREATORS.COM
10-16
WHAT WAS HE DOING?
TRYING TO READ THE WARNING LABEL
PARKER

WIZARD OF ID by, Brant Parker and Johnny Hart

Multidisciplinary Approach to System Safety

BAE SYSTEMS

- What is a multidisciplinary approach to system safety?
  - Consulting with professionals from other disciplines
    - To gain knowledge when needed
    - To ensure end-to-end system safety
    - Keep abreast of the new technologies
    - Eliminate conflicting requirements



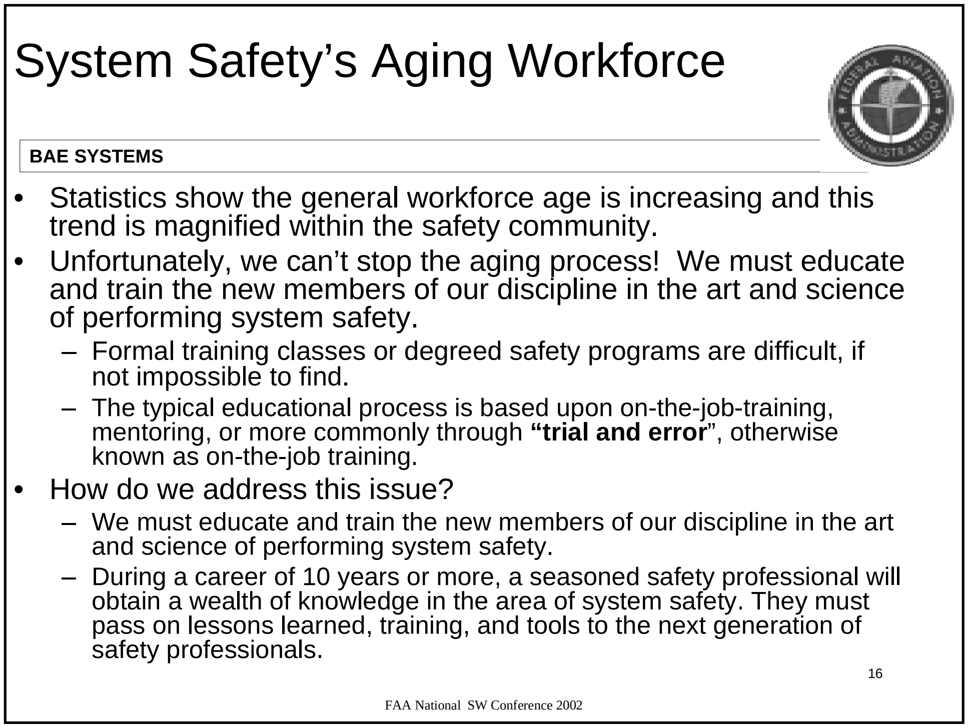
Multidisciplinary Approach to System Safety

BAE SYSTEMS

- How can conflicting requirements occur?
  - Tight schedules
  - Complex systems
  - Complex systems within systems
  - Poor requirements validation
  - Poor requirements verification
  - **Lack of communication between the various engineering disciplines**

15

FAA National SW Conference 2002



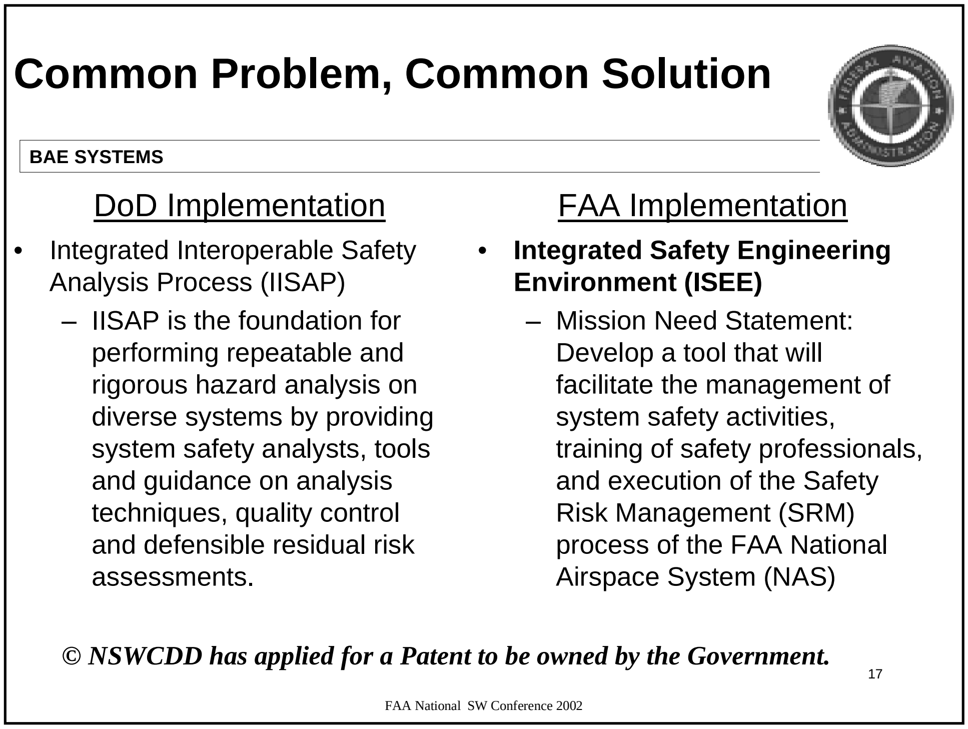
System Safety's Aging Workforce

BAE SYSTEMS

- Statistics show the general workforce age is increasing and this trend is magnified within the safety community.
- Unfortunately, we can't stop the aging process! We must educate and train the new members of our discipline in the art and science of performing system safety.
  - Formal training classes or degreed safety programs are difficult, if not impossible to find.
  - The typical educational process is based upon on-the-job-training, mentoring, or more commonly through **"trial and error**", otherwise known as on-the-job training.
- How do we address this issue?
  - We must educate and train the new members of our discipline in the art and science of performing system safety.
  - During a career of 10 years or more, a seasoned safety professional will obtain a wealth of knowledge in the area of system safety. They must pass on lessons learned, training, and tools to the next generation of safety professionals.

16

FAA National SW Conference 2002



Common Problem, Common Solution

BAE SYSTEMS

DoD Implementation

- Integrated Interoperable Safety Analysis Process (IISAP)
  - IISAP is the foundation for performing repeatable and rigorous hazard analysis on diverse systems by providing system safety analysts, tools and guidance on analysis techniques, quality control and defensible residual risk assessments.

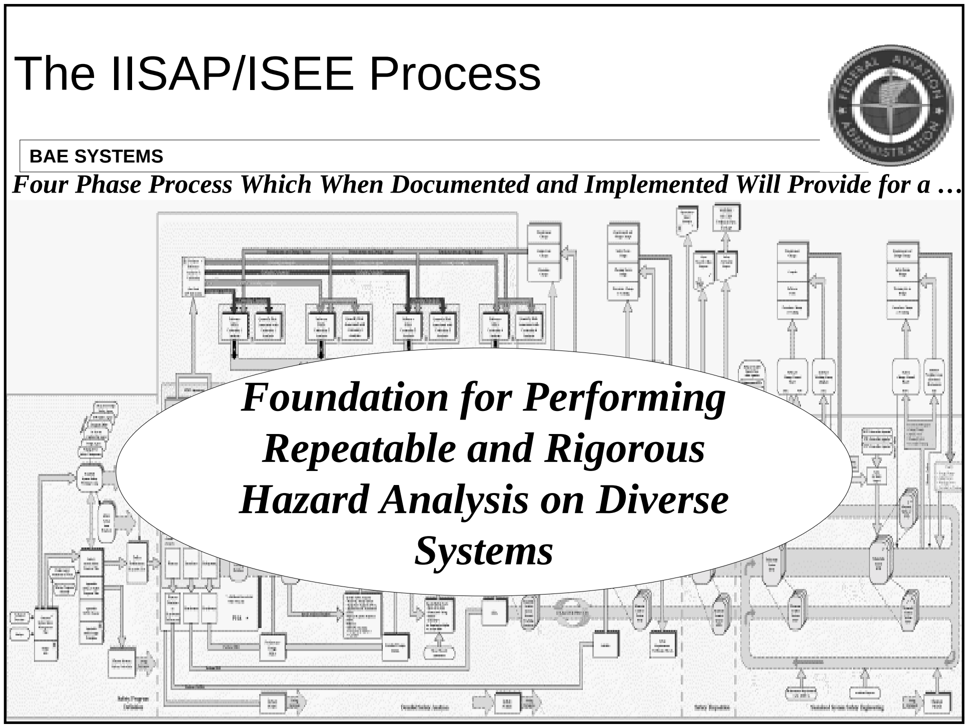
FAA Implementation

- **Integrated Safety Engineering Environment (ISEE)**
  - Mission Need Statement: Develop a tool that will facilitate the management of system safety activities, training of safety professionals, and execution of the Safety Risk Management (SRM) process of the FAA National Airspace System (NAS)

© NSWCDD has applied for a Patent to be owned by the Government.

17

FAA National SW Conference 2002

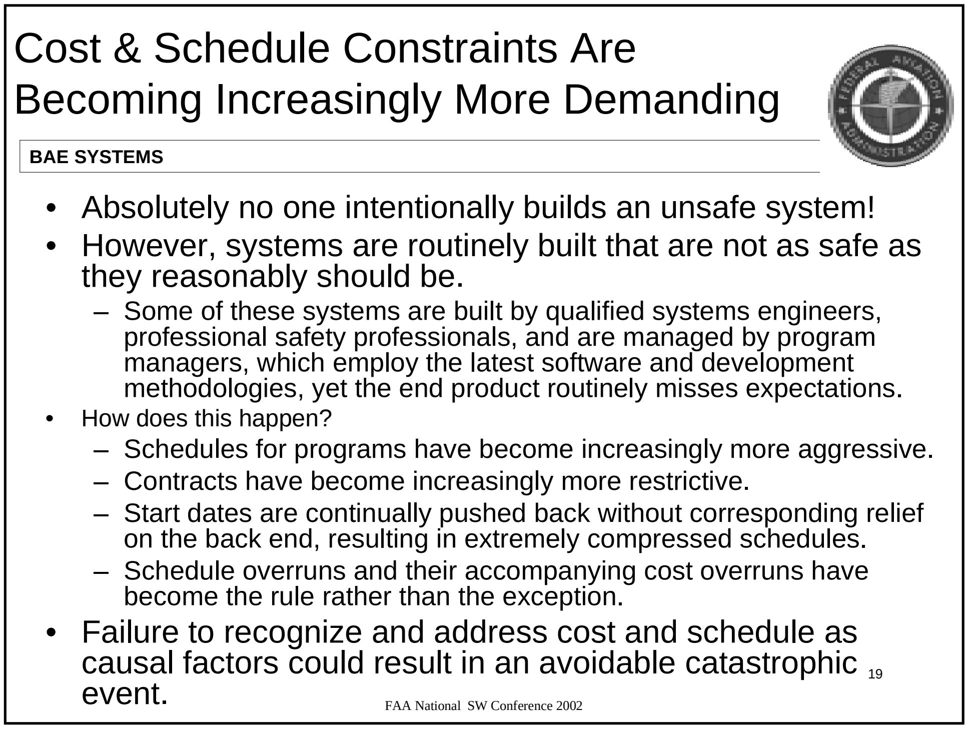


The IISAP/ISEE Process

BAE SYSTEMS

Four Phase Process Which When Documented and Implemented Will Provide for a …

Foundation for Performing Repeatable and Rigorous Hazard Analysis on Diverse Systems



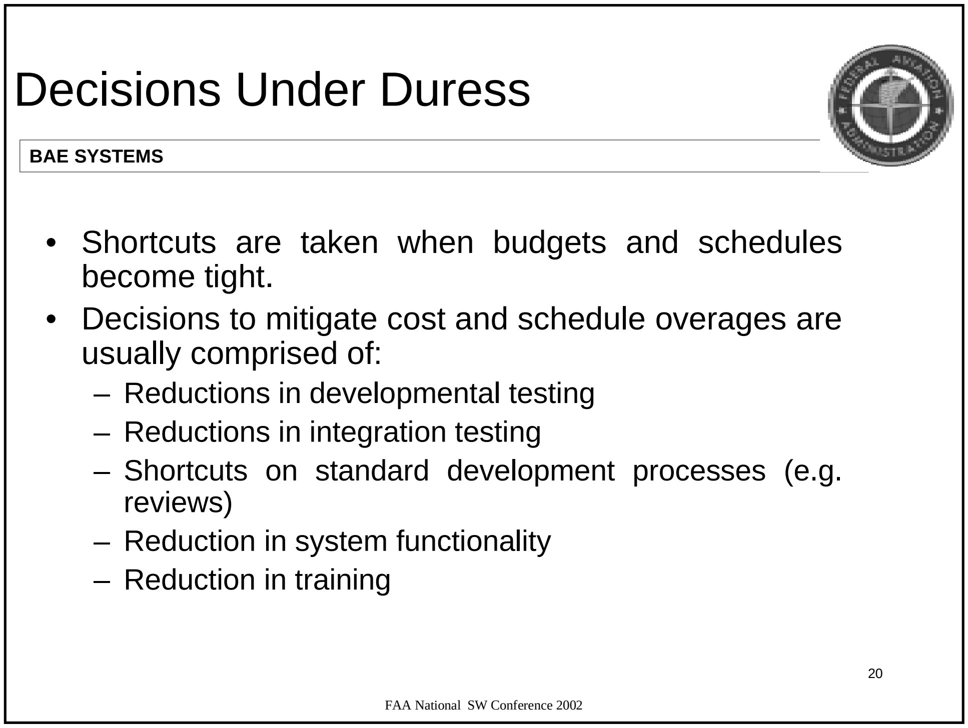
Cost & Schedule Constraints Are Becoming Increasingly More Demanding

BAE SYSTEMS

- Absolutely no one intentionally builds an unsafe system!
- However, systems are routinely built that are not as safe as they reasonably should be.
  - Some of these systems are built by qualified systems engineers, professional safety professionals, and are managed by program managers, which employ the latest software and development methodologies, yet the end product routinely misses expectations.
- How does this happen?
  - Schedules for programs have become increasingly more aggressive.
  - Contracts have become increasingly more restrictive.
  - Start dates are continually pushed back without corresponding relief on the back end, resulting in extremely compressed schedules.
  - Schedule overruns and their accompanying cost overruns have become the rule rather than the exception.
- Failure to recognize and address cost and schedule as causal factors could result in an avoidable catastrophic event.

19

FAA National SW Conference 2002



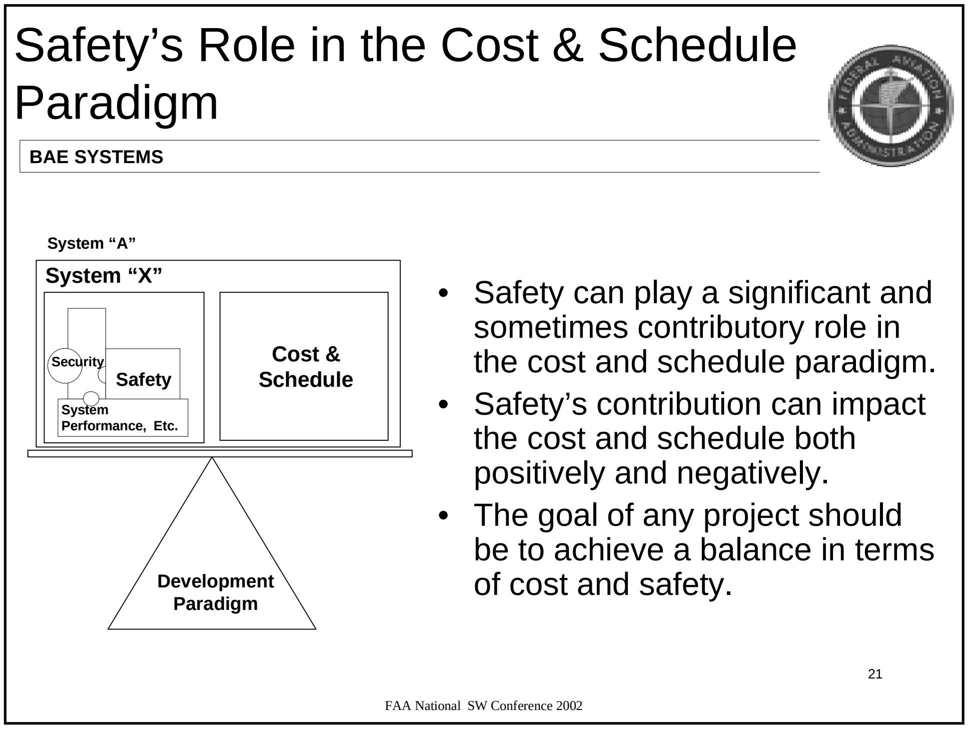
Decisions Under Duress

BAE SYSTEMS

- Shortcuts are taken when budgets and schedules become tight.
- Decisions to mitigate cost and schedule overages are usually comprised of:
  - Reductions in developmental testing
  - Reductions in integration testing
  - Shortcuts on standard development processes (e.g. reviews)
  - Reduction in system functionality
  - Reduction in training

20

FAA National SW Conference 2002



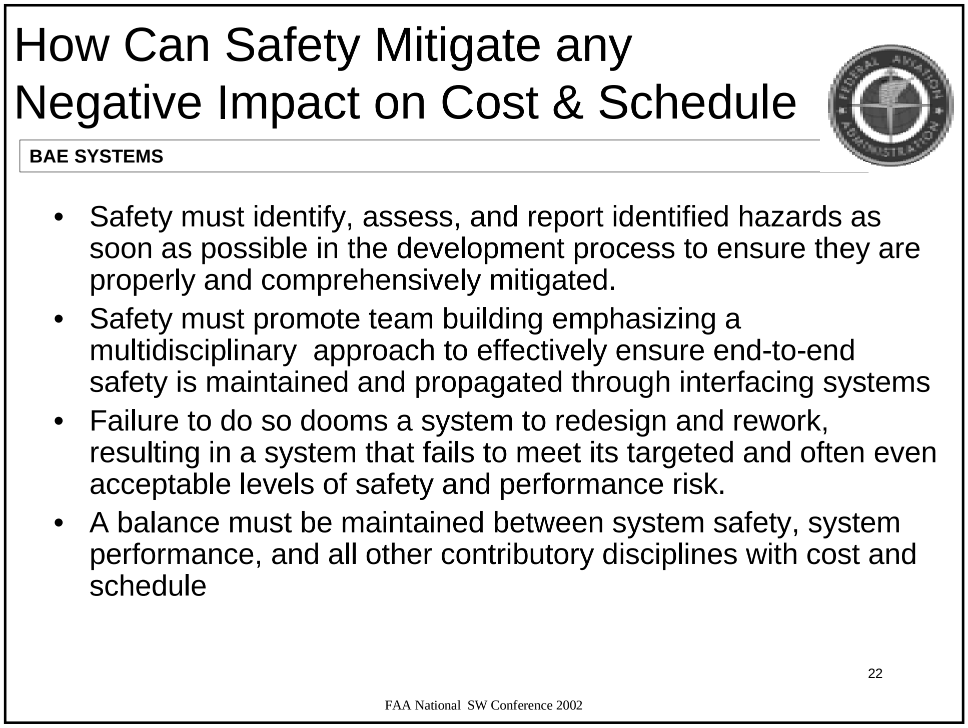
Safety's Role in the Cost & Schedule Paradigm

BAE SYSTEMS

- Safety can play a significant and sometimes contributory role in the cost and schedule paradigm.
- Safety's contribution can impact the cost and schedule both positively and negatively.
- The goal of any project should be to achieve a balance in terms of cost and safety.

21

FAA National SW Conference 2002



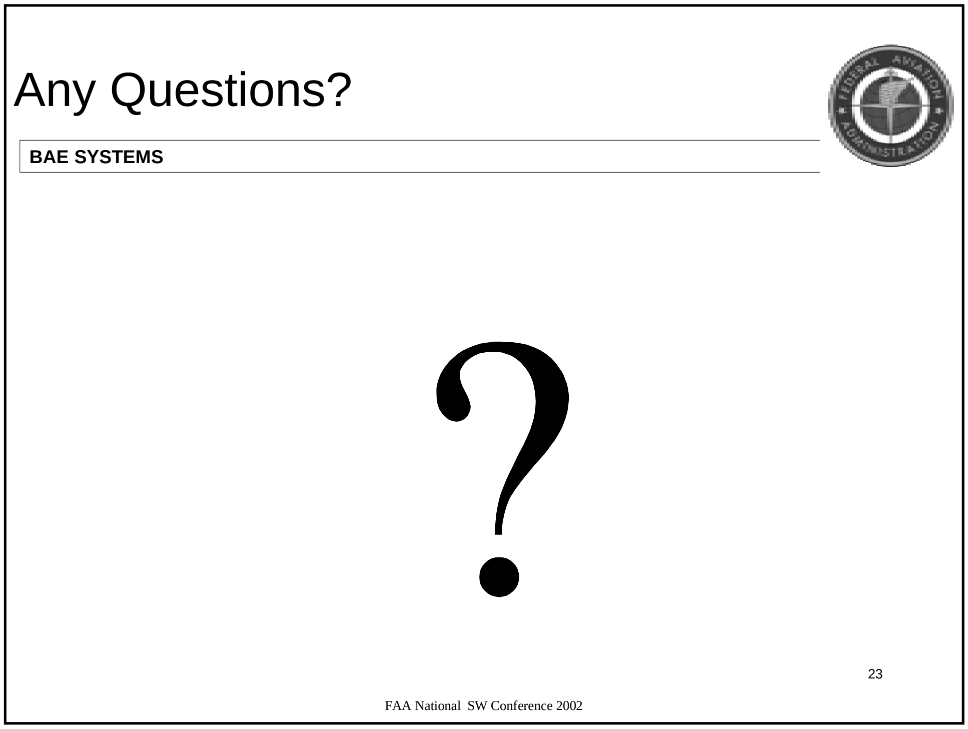
How Can Safety Mitigate any Negative Impact on Cost & Schedule

BAE SYSTEMS

- Safety must identify, assess, and report identified hazards as soon as possible in the development process to ensure they are properly and comprehensively mitigated.
- Safety must promote team building emphasizing a multidisciplinary approach to effectively ensure end-to-end safety is maintained and propagated through interfacing systems
- Failure to do so dooms a system to redesign and rework, resulting in a system that fails to meet its targeted and often even acceptable levels of safety and performance risk.
- A balance must be maintained between system safety, system performance, and all other contributory disciplines with cost and schedule

22

FAA National SW Conference 2002



Any Questions?

BAE SYSTEMS

?

23

FAA National SW Conference 2002